WHAT IS CLAIMED IS:

1. A document printing program comprising the codes of:

obtaining a print requirement associated with a document file; and

compulsory executing the print requirement when the document file is printed out.

2. The document printing program as claimed in claim 1, wherein the print requirement is compulsory enforced by executing a printing process with the print requirement when the document file being encoded is decrypted.

3. The document printing program as claimed in claim 2, further comprising the codes of:

obtaining a decryption key for the document file being encrypted;

decrypting the document file based on the obtained decryption key;

obtaining the print requirement associated with the document file; and

executing a printing process so as to satisfy the obtained print request.

4. The document printing program as claimed in claim 3, wherein the print requirement is obtained from the decrypted document file.

5. The document printing program as claimed in claim 4, wherein a password corresponding to an encryption key used to encrypt the document file is obtained from a user, and an decryption key is generated by the password.

6. The document printing program as claimed in claim 5, wherein a parameter, which is internally maintained or generated, is used to generate the decryption key.

7. The document printing program as claimed in claim 3, wherein the print requirement associated with the document file is obtained from a server through the network.

8. The document printing program as claimed in claim 7, further comprising the codes of:

conducting a user authentication with respect to the server;

obtaining the print requirement of an authenticated user

9. The document printing program as claimed in claim 8, wherein a parameter corresponding to an encryption key used to encrypt the document file is obtained from a server through a network, and an decryption key is obtained from the parameter.

10. The document printing program as claimed in claim 9, wherein a parameter, which is internally maintained or generated, is used to generate the decryption key.

11. The document printing program as claimed in claim 9, wherein a parameter included in the document file is used to generate the decryption key.

12. A document protecting program comprising the codes of:
obtaining an encryption key used to encrypt a document file;
associating print requirement with the document file; and
encrypting the document file by the encryption key.

13. The document protecting program as claimed in claim 12, wherein the document file and the print requirement are associated with each other by providing the print requirement to the document file and then encrypting the document file with the print requirement.

14. The document protecting program as claimed in claim 13, wherein an encryption key is generated based on a password input by a user.

15. The document protecting program as claimed in claim 14, wherein a parameter internally maintained and generated is used to generate the encryption key.

16. The document protecting program as claimed in claim 12, wherein the print requirement associated with the document file is registered to a server through a network.

17. The document protecting program as claimed in claim 16, wherein the print requirement is registered as a part of an ACL associated with the document file.

18. The document protecting program as claimed in claim 17, wherein an encryption key user to encrypt is registered to the server.

19. The document protecting program as claimed in claim 18, wherein a parameter used to generate an encryption key used to encrypt is registered to the server.

20. The document protecting program as claimed in claim 18, wherein a parameter used to generate an encryption key used to encrypt is provided to a part of the document.

21. A document protecting system comprising:

a distributor terminal implementing a document protecting program comprising the codes of:

a part obtaining an encryption key to encrypt a document file;

a part associating a print request to the document file; and

a part encrypting the document file by the encryption key, and

a user terminal implementing a document printing program comprising the codes of:

a part obtaining a decryption key of document file being encrypted;

a part decrypting the document file based on the obtained decryption key;

a part obtaining a print requirement associated with the document file; and

a part executing a printing process so as to satisfy the print requirement.

22. A document protecting system comprising:

a server implementing a document protecting program comprising the codes of:

obtaining an encryption key used to encrypt a document file;

associating a print requirement with the document file; and

encrypting the document file by the encryption key, and

a user terminal comprising the codes of:

obtaining a decryption key of a document being encrypted;

obtaining a print requirement associated with the document; and

executing a printing process so as to satisfy the obtained print requirement.

23. A document printing program comprising the codes of:

obtaining decryption key of a document file being encrypted;

decrypting the document based on the decryption key;

obtaining a print requirement associated with the document file from a server through a network; and

executing a printing process satisfying the print requirement.

24. The document printing program as claimed in claim 23, further comprising the codes of:

conducting a user authentication with respect to the server; and

obtaining print requirement of a user being authenticated from an ACL associated with security attributes of the document file so as to define for each organization unit.

25. The document printing program as claimed in claim 24, wherein a security attribute database, that registers the security attributes of the document file being encrypted by associating with the document file.

26. The document printing program as claimed in claim 25, wherein the security attributes include a document category and a secret level.

27. The document printing program as claimed in claim 23, further comprising the codes of:

conducting a user authentication with respect to the server; and

obtaining a security policy, which is provided by associating the print requirement of a user being authorized with the security attributes and a user type.

28. The document printing program as claimed in claim 27, wherein a security attribute database, which registers the security attributes of the document file being encrypted by associating with the document file, is provided in the server.

29. The document printing program as claimed in claim 28, wherein the security attributes include a document category and a security level, and the user type includes a category and a level.

30. The document printing program as claimed in claim 24, wherein a parameter corresponding to an encryption key used to encrypt the document file is obtained from a server through a network, and the decryption key is generated from the parameter.

31. The document printing program as claimed in claim 30, wherein the parameter internally maintained and generated is used to generate the decryption key.

32. The document printing program as claimed in claim 30, wherein the parameter included in the document file is used to generate the decryption key.

33. A document protecting program comprising the codes of:

obtaining an encryption key user to encrypt a document file;

registering information indicating a print requirement of the document file to a server by associating with the document file through the network; and

encrypting the document file by the encryption key.

34. The document protecting program as claimed in claim 33, wherein security attributes indicating the print requirement is registered to a server by associating with the document file.

35. The document protecting program as claimed in claim 34, wherein a security attribute database, which register the security attributes by associating with the document file, is provided in the server.

36. The document protecting program as claimed in claim 35, wherein the security attributes include a document category and a secret level.

37. The document protecting program as claimed in claim 33, herein an encryption key used to encrypt is registered to the server.

38. The document protecting program as claimed in claim 33, wherein a parameter used to generate the encryption key used to encrypt is registered to the server.

39. The document protecting program as claimed in claim 37, wherein a parameter used to generate the encryption key used to encrypt is provided to a part of the document file.

40. A document protecting system comprising:

a distributor terminal implementing a document protecting program comprising the codes of:

a part obtaining an encryption key to encrypt a document file;

registering information indicating a print requirement of the document file to a server by associating with the document file through a network; and

a part encrypting the document file by the encryption key, and

a user terminal implementing a document printing program comprising the codes of:

a part obtaining a decryption key of the document file being encrypted;

a part decrypting the document file based on the decryption key;

a part obtaining a print requirement associated with the document file from a server through the network; and

a part executing a printing process satisfying the print requirement.

41. A document protecting system comprising:

a server implementing a document protecting program comprising the codes of:

a part obtaining an encryption key used to encrypt a document file;

a part registering information indicating a print requirement of the document file; and

a part encrypting the document file by the encryption key, and

a user terminal implementing a document printing program comprising the codes of:

a part obtaining a decryption key of the document file being encrypted;

a part decrypting the document file based on the decryption key;

a part obtaining a print requirement associated with the document file from a server through a network; and

a part executing a printing process satisfying the print requirement.

42. A document printing apparatus comprising:

a part obtaining a user attribute of a user who prints out a document file;

a part obtaining a document attribute of the document file;

a part obtaining a print requirement by searching for a security policy ruling a print allowed/denied and a print requirement based on the user attribute and the document attribute; and

a part enforcing the print requirement when the document file is printed out.

43. The document printing apparatus as claimed in claim 42, wherein the security policy is internally provided.

44. The document printing apparatus as claimed in claim 42, wherein the security policy arranged in a server is referred.

45. The document printing apparatus as claimed in claim 44, wherein the security policy is referred, and a printing process is executed for the document file.

46. The document printing apparatus as claimed in claim 45, wherein a document printing program comprises the codes of:

obtaining a decryption key of the document file being encrypted;

decrypting the document file based on the decryption key;

obtaining the print requirement from the server through the network; and

executing the printing process satisfying the print requirement.

47. The document printing apparatus claimed in claim 46, wherein a security attribute database, which registers the document attribute by associating with the document file, is provided in the server.

48. The document printing apparatus claimed in claim 47, wherein the document attribute includes a document category and a security level, and the user attribute includes a category and a level.

49. The document printing apparatus claimed in claim 46, wherein a parameter corresponding to an encryption key used to encrypting the document file is obtained from the server through the network, and the decryption key is generated from the parameter.

50. The document printing apparatus claimed in claim 49, wherein the parameter internally maintained or generated is used to generate the decryption key.

51. The document printing apparatus claimed in claim 49, wherein the parameter included in the document file is used to generate the decryption key.

52. An electronic file management apparatus comprising:

an electronic file storage area storing an electronic file;

an electronic file managing part additionally providing access authorization information to the electronic file and storing the electronic file in the electronic file storage area; and

a secured electronic file outputting part outputting a secured electronic file in that the electronic file is encrypted and secured, in response to an access request of the electronic file.

53. The electronic file management apparatus as claim in claim 52, wherein when the electronic file managing part receives a storing request of the electronic file, the electronic file managing part obtains the secured electronic file secured by encrypting the electronic file, and associates the electronic file with the secured electronic file to store in the electronic file storing area.

54. The electronic file management apparatus as claimed in claim 52, wherein the electronic file receives a storing request, the electronic file obtains the secured electronic file secured by encrypting the electronic file, and stores the secured electronic file in the electronic file storing file, instead of storing the electronic file.

55. The electronic file management apparatus as claimed in claim 52, wherein when the secured electronic file outputting part receives an access request of the electronic file, the secured electronic file outputting part obtains the secured electronic file secured by encrypting the electronic file, and outputs the secured electronic file.

56. The electronic file management apparatus as claimed in claim 52, wherein when the electronic file managing part receives a storing request of the electronic file, the electronic file managing part accepts the electronic file and the secured electronic file, and associates the electronic file with the secured electronic file to store in the electronic file storing area.

57. The electronic file management apparatus as claimed in claim 52, further comprising a secured electronic file obtaining part obtaining the secured electronic file by sending the electronic file and the access authorization to an external part for encrypting the electronic file, and providing the secured electronic file to the electronic file managing part.

58. The electronic file management apparatus as claimed in claim 52, wherein the secured electronic file is encrypted based on the access authorization information.

59. The electronic file management apparatus as claimed in claim 52, wherein when the secured electronic file outputting part receives an access request to the electronic file before the electronic file is secured, the secured electronic file outputting part determines whether or not the access authorization is allowed to the electronic file before being secured, and denying the access request.

60. A program for causing a computer to manage an electronic file, program comprising the codes of:

additionally providing access authorization information to the electronic file and storing the electronic file in an electronic file storage area; and

outputting a secured electronic file in that the electronic file is encrypted and secured, in response to an access request of the electronic file.

61. A file access controlling method comprising:

managing an electronic so as to provide a secured electronic file in that an electronic file is secured by encrypting based on access authorization information, in response to an access request;

obtaining the secured electronic file in response to a process request for the electronic file; and

controlling a process with respect to the secured electronic file that is decrypted in accordance with the access authorization information when the secured electronic file is decrypted.

62. The file access controlling method as claimed in claim 61, further comprising:

managing electronic file identification information identifying the electronic file, a key for decrypting the secured electronic file, and the access control information;

obtaining user authentication information for authenticating a user who conducted the process request, the electronic file identification information, and the process type when receiving the process request;

determining whether or not to allow or deny the process based on the access authorization information when the user authentication is succeeded;

obtaining a process requirement indicated when allowing the process and the key based on a determination result;

decrypting the secured electronic file by using the key; and

controlling the process in accordance with the process requirement.

63. An access control server connectable to a network, comprising:

an electronic data receiving part receiving electronic data from an author terminal of an author of the electronic data through the network;

a workflow information receiving part receiving workflow information including information showing a data type of the electronic data;

a template storing part storing at least one access authorization template showing an access authorization for each user type with respect to the electronic data for each data type of the electronic data;

a template retrieving part retrieving an access authorization template corresponding to data type information of the electronic data included in the workflow information, from at least one access authorization template being stored in the template storing part; and

an access authorization information generating part generating the access authorization information showing the access authorization of each user with respect to electronic data by inserting the user ID of each user to an access authorization template.

64. The access control server as claimed in claim 63, further comprising:

an approval information receiving part receiving approval information showing that an issuance of the electronic data is approved by an approver;

an access restriction data generating part generating access restriction data by applying an access restriction to the electronic data based on the access restriction information; and

a data sending part sending the access restriction data through the network.

65. The access control server as claimed in claim 64, wherein the template storing part stores the access authorization template setting the author of the electronic data, an approver of the electronic data, and a user whom the access restriction data is sent to, as the user type.

66. The access control server as claimed in claim 64, wherein the access control data generating part applies the access restriction to the electronic data and generates the access restriction data based on a security policy stored in said access control server itself.

67. The access control server as claimed in claim 64, wherein the access restriction data generating part applies the access restriction to the electronic data, converts a data format, and generates the access restriction data.

68. An electronic data issuance workflow processing method in an access control server for conducting an access control to an electronic data, said access control server connectable to a network, said method comprising the steps for:

an electronic data step receiving step for the access control server to receive electronic data from an author terminal of an author of the electronic data through the network;

a workflow information receiving step for the access control server to receive workflow information including information showing a data type of the electronic data;

a template storing step for the access control server to store at least one access authorization template showing an access authorization for each user type with respect to the electronic data for each data type of the electronic data;

a template retrieving step for the access control server to retrieve an access authorization template corresponding to data type information of the electronic data included in the workflow information, from at least one access authorization template being stored in the template storing part; and

an access authorization information generating step for the access control server to generate the access authorization information showing the access authorization of each user with respect to electronic data by inserting the user ID of each user to an access authorization template.

69. The electronic data issuance workflow processing method as claimed in claim 68, further comprising the steps for:

an approval information receiving step for the access control server to receive approval information showing that an issuance of the electronic data is approved by an approver;

an access restriction data generating step for the access control server to generate access restriction data by applying an access restriction to the electronic data based on the access restriction information after the approval information is received; and

a data sending step for the access control server to send the access restriction data through the network.

70. The electronic data issuance workflow processing method as claimed in claim 68, further comprising the steps for:

an access restriction data generating step for the access control server to generate access restriction data by applying an access restriction to the electronic data based on the access restriction information;

an approval information receiving step for the access control server to receive approval information showing that an issuance of the electronic data is approved by an approver;

a data sending step for the access control server to send the access restriction data through the network.

71. The electronic data issuance workflow processing method as claimed in claim 69, wherein the template storing step stores the access authorization template setting the author of the electronic data, an approver of the electronic data, and a user whom the access restriction data is sent to, as the user type.

72. The electronic data issuance workflow processing method as claimed in claim 69, wherein the access control data generating step applies the access restriction to the electronic data and generates the access restriction data based on a security policy stored in said access control server itself.

73. The electronic data issuance workflow processing method as claimed in claim 69, wherein the access restriction data generating step applies the access restriction to the electronic data, converts a data format, and generates the access restriction data.

74. A program for causing an access control server to conduct an access control to an electronic data, said access control server connectable to a network, program comprising the codes of:

an electronic data code receiving code for the access control server to receive electronic data from an author terminal of an author of the electronic data through the network;

a workflow information receiving code for the access control server to receive workflow information including information showing a data type of the electronic data;

a template storing code for the access control server to store at least one access authorization template showing an access authorization for each user type with respect to the electronic data for each data type of the electronic data;

a template retrieving code for the access control server to retrieve an access authorization template corresponding to data type information of the electronic data included in the workflow information, from at least one access authorization template being stored in the template storing part; and

an access authorization information generating code for the access control server to generate the access authorization information showing the access authorization of each user with respect to electronic data by inserting the user ID of each user to an access authorization template.

75. The program claimed in claim 74, further comprising the codes of:

an approval information receiving code for the access control server to receive approval information showing that an issuance of the electronic data is approved by an approver;

an access restriction data generating code for the access control server to generate access restriction data by applying an access restriction to the electronic data based on the access restriction information after the approval information is received; and

a data sending code for the access control server to send the access restriction data through the network.

76. The program claimed in claim 74, further comprising the codes for:

an access restriction data generating code for the access control server to generate access restriction data by applying an access restriction to the electronic data based on the access restriction information;

an approval information receiving code for the access control server to receive approval information showing that an issuance of the electronic data is approved by an approver;

a data sending code for the access control server to send the access restriction data through the network.

77. The program as claimed in claim 75, wherein the template storing code stores the access authorization template setting the author of the electronic data, an approver of the electronic data, and a user whom the access restriction data is sent to, as the user type.

78. The program as claimed in claim 75, wherein the access control data generating code applies the access restriction to the electronic data and generates the access restriction data based on a security policy stored in said access control server itself.

79. The program as claimed in claim 75, wherein the access restriction data generating code applies the access restriction to the electronic data, converts a data format, and generates the access restriction data.